PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G11B 20/00, G06F 1/00 — A1

(11) International Publication Number: WO 98/54713

(43) International Publication Date: 3 December 1998 (03.12.98)

(21) International Application Number: PCT/IB98/00800

(22) International Filing Date: 25 May 1998 (25.05.98)

(30) Priority Data:
97303706.2 30 May 1997 (30.05.97) EP
(34) Countries for which the regional or international application was filed: GB et al.

(71) Applicant: Ç-DILLA LIMITED [GB/GB]; Woodley House, Crockhamwell Road, Woodlex, Reading, Berkshire RG5 3JP (GB).

(72) Inventor: NEWMAN, Peter, A.; Woodley House, Crockhamwell Road, Woodley RG5 3JP (GB).

(74) Agent: FAESSEN, Louis, M., H.; Internationaal Octrooibureau B.V., P.O. Box 220, NL-5600 AE Eindhoven (NL).

(81) Designated States: AL, AM, AU, AZ, BA, BB, BG, BR, BY, CA, CN, CU, CZ, EE, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, RO, RU, SD, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD FOR COPY PROTECTING A RECORD CARRIER, COPY PROTECTED RECORD CARRIER AND MEANS FOR DETECTING ACCESS CONTROL INFORMATION

(57) Abstract

A method for copy protecting a record carrier is disclosed, in which method the copy protected record carriers are provided with a pattern of logical errors which cannot be corrected by the error correcting rules predefined for said record carrier. The pattern of logical errors represents access control information. The logical errors are generated during decoding the bit sequence read from the record carrier. Bit errors may be positioned in the bit sequence so as to counteract de-interleaving which is part of an error decoding process in a reading device and accumulate in error words which are uncorrectable. Also a method for detecting access control information and a retrieval arrangement are disclosed, which retrieval arrangement serves to detect the access control information by selecting at least one error location, but not all error locations on the record carrier, and verifying the presence of an error by reading the selected error location via the reading means.

AM

Method for copy protecting a record carrier, copy protected record carrier and means for detecting access control information.

The invention relates to a method for copy protecting a record carrier having information stored thereon according to predetermined formatting and error correcting rules, comprising the steps of creating an image file comprising main information, generating access control information for controlling the access to the main information, producing a master carrier in dependence on the image file and the access control information, which producing comprises the steps of creating a bit sequence by applying the formatting and error correcting rules to the image file and translating the bit sequence into a physical pattern of marks, and multiplicating the record carrier using the master carrier.

The invention further relates to a copy protected record carrier having a bit sequence stored thereon representing information according to predetermined formatting and error correcting rules, the information comprising main information and access control information for controlling the access to the main information.

The invention further relates to a method for detecting access control information on such a copy protected record carrier.

The invention further relates to a retrieval arrangement for retrieving information from such a copy protected record carrier, the arrangement comprising reading means for reading the record carrier, the reading means comprising a read unit for extracting a bit sequence stored on the record carrier and an error correcting unit for processing the bit sequence.

A system for copy protecting a record carrier, a copy protected record carrier and a reading arrangement are known from EP-0545472 (document D1 in the list of related documents). The known record carrier comprises a prearranged guiding track, a so-called pregroove. In the track determined by the pregroove, information which is written in a predefined manner is represented by optically readable patterns which are formed by variation of a first physical parameter, such as the height of the scanned surface. The pregroove has variations in a second physical parameter, such as an excursion in a transverse direction, also denoted as wobble. Pregroove wobble is FM-modulated and this modulation

described in the opening paragraph is characterized in that the arrangement comprises access control means for controlling the access to the information, which access control means are embodied so as to detect the access control information by selecting at least one error location, but not all error locations, which error location(s) should have a logical error according to the error pattern, and by verifying the presence of an error by reading the selected error location via the reading means. This is advantageous in that selecting a few error locations from an available larger number results in a fast response for the access control means. Reading a sector having errors might take up to 30 seconds on a standard reading device, such as a CD-ROM drive, due to automatic retries. Also selecting different locations for each access control session increases the difficulties for a malicious party in mimicking the access control process.

It is to be noted, that WO 95/03655 (document D3) describes a CD PROM encryption system, in which the information on a CD-ROM is encrypted by a key, which key is programmed into the CD-ROM after manufacture by damaging selected sectors to be unreadable by conventional read systems. The selected sectors are physically damaged by a high power laser. Record carriers are individually enabled by having a specific key for a certain user or group of users.

The invention is also based on the following recognition. Physically damaging selected parts of a record carrier leads to corrupted physical marks. When reading such damaged parts a read head may lose the track, or the translation from the read signal to a bit sequence may be disrupted or lose synchronisation, which all result in an uncontrollable number of errors. Moreover, physical damage may be easily detected from physical parameters and may be mimicked by a malicious party by physical means. Also, physically damaging sectors increases the production cost. The invention is based on a logical pattern of errors, which does not increase production cost and allows precise control of the resulting errors. In addition the inventors have had the insight, that physical errors cannot be used for generating errors in a limited part of the retrieved information, as they are similar to burst errors, which type of error is spread widely due to de-interleaving steps usually applied to the bit sequence in an error correcting and deformatting process for retrieving the information. Therefore, an embodiment of the copy protected record carrier is characterized in that, while the bit sequence comprises information bits and error correction bits, the information bits comprise the bit errors and/or in that the bit errors are located so as to accumulate in an error word uncorrectable by an error word correcting rule when reproducing. This is advantageous in that the bit errors are concentrated in error words

spreading over more locations due to de-interleaving rules will be detected.

Further advantageous, preferred embodiments of the copy protected record carrier, the retrieval arrangement and methods according to the invention are given in the further dependent claims.

These and other aspects of the invention will be apparent from and elucidated further with reference to the embodiments described by way of example in the following description and with reference to the accompanying drawings, in which

Figure 1 shows a copy protected record carrier

Figure 2 shows a logical map of the recording area of a copy protected record carrier

Figure 3 shows an error correcting unit

Figure 4 shows a bit error pattern

Figure 5 shows an arrangement for retrieving information from a copy protected record carrier

Figure 6 shows a schematic diagram for copy protecting a record carrier

Fig. 1 shows schematically a disc-shaped copy protected record carrier 1. The record carrier comprises a track 9 for storing information, which track is arranged in a helical pattern of windings around a central hole 10. The windings may also be arranged concentrically in lieu of helically. The record carrier 1 is of an optically readable type in which a transparent substrate is covered by a recording layer and a protective layer, such as the well-known Compact Disc (CD). Information on the information carrier is represented by patterns of optically readable marks. For example, the position and/or the length of the marks then represent a binary information signal. The marks may be made by presses, as is customary for read-only CD's, such as CD-ROM on which embossed pits and lands between the pits represent the information. The invention can be used for any type of record carrier, on which information is recorded according to predetermined error correcting rules, such as the high density optical disc DVD (Digital Versatile Disc), optical tape or magnetic tape for digital video. The track 9 comprises the marks and is scannable by a read head for reading the stored information. The marks represent a bit sequence according to a channel code, such as EFM for CD (Eight to Fourteen Modulation). The bit sequence represents information

decoding step after reading the marks. Applying errors on a higher system level before the error encoding, e.g. by intentionally changing the EDC (error detection codes) in a sector or a sector header in CD-ROM, may be easily mimicked by a malicious party, because the formatting process for higher levels is usually performed via software and therefore accessible for manipulation. An operational, but illegal, copy comprising the higher level errors may be made with standard recording devices and (adapted) software in the connected computer system, e.g. a bit copying program available for making copies of audio CD's.

As burst errors will occur due to dirt or scratches on the surface of a record carrier, error correcting rules, e.g. of CD, are especially designed for correcting burst errors by applying interleaving before storing and de-interleaving after reading. The bit errors constituting such a burst error will be mixed with a far larger number of other bits from the bit sequence by de-interleaving rules which are part of the formatting and error correcting rules. A number of consecutive bit errors sufficient to cause the uncorrectable errors has to be longer than the longest correctable burst error. The error correcting rules are described with Figure 3. In a preferred embodiment only selected bits of the bit sequence show errors, which bits are selected so as to accumulate by de-interleaving, which de-interleaving is part of the formatting and error correcting rules. This results in a location on the record carrier showing a high concentration of errors, while adjoining locations show only a few or no bit errors. An example of bit errors is described with Figure 4. Usually error correcting rules and especially (de)interleaving rules will operate on symbols, e.g. on bytes of 8 bits, while the error correcting process is applied to error words of a number of symbols accumulated by de-interleaving. The error symbols are selected to accumulate during de-interleaving to an uncorrectable number in one or a few error words.

An effective way of applying bit errors is to invert each bit from a selected symbol in the original bit sequence without errors, which selected symbol is to be provided with a bit error. Alternatively the bit errors may be applied to the symbols, when said symbols are translated into the pattern of physical marks, e.g. using a controllable EFM encoder. For said symbols the EFM encoder might be controlled to change some of the physical marks to be different from the originally intended marks based on the bit sequence without errors. Preferably the resulting physical marks comply with the constraints specified for the physical marks, as this assures reliable functioning of the reading and decoding process.

Figure 2 shows a logical map of the recording area of a copy protected record carrier. The recording area is subdivided in addressable sectors from the top at address 00 up

consecutively stored on the record carrier, indicated by the column bytes numbered 0 to 31, comprising twelve data bytes 0-11, four C2 error correcting bytes 12-15, again twelve information bytes 16-27 and four C1 error correcting bytes. The odd bytes are delayed by one cycle in a first delay unit 31, and the resulting error words of 32 bytes are error corrected by the C1 unit 32. The C1 unit can correct one byte error and detect all 2 and 3 byte errors, while 4-32 byte errors are detected with a very low failure rate. If the C1 unit detects un uncorrectable error, it will flag all bytes to be unreliable. The output of the C1 unit is delayed by a second delay unit 33, delaying byte 0 by 27 * 4 = 108 frames, byte 1 by 26 * 4 = 102 frames etc. The output of the second delay unit 33 constitutes a second error word, which is error corrected by the C2 unit. The C2 unit usually corrects up to 2 errors, but may correct up to 4 bytes by erasure if the C1 unit flags all detected errors. The output of the C2 unit is descrambled by descramble unit 35. The described functions are the complement of inverse functions in the encoder, all functions being well-known from the CD system and described in detail in document D2. According to the invention a logical error result from bit errors being uncorrectable, therefore bit errors must be present in the input frames accumulating to at least 2 but preferably 3 or more errors in the error words on the input of the C1 unit. Also at least 3 but preferably at least 5 errors should be present in at least one second error word on the input of the C2 unit. For 5 errors in one second error word this requires at least 17 consecutive error-flagged output frames of C1, having errors in a group of 5 consecutively numbered information bytes. For example, errors in byte 0 in frame 0 will accumulate at the input of C2 with errors in byte 2 in frame 8 and errors in byte 4 in frame 16. For creating a cluster of logical errors within a specified data unit, such as a sector in the CD system, preferably more bit errors than the above minimum of 5 errors in 17 consecutive frames should be applied. A further error correcting layer, such as used in CD-ROM for error correcting within a sector, may correct some logical errors uncorrectable by the above error correcting rules. Therefore a larger number of logical errors should be included. An embodiment achieving a safe margin without risk of spreading the errors over a large area has errors in all of the first or second twelve consecutively numbered information bytes. Said errors will spread due to the second delay unit over 12 * 4 = 48 frames and 1 additional frame because of the first delay unit, and having 24 consecutive frames with errors, over 48 + 1 + 24 = 73 frames. As a frame comprises 24 information bytes this affects 73 * 24 bytes = 1752 bytes, which is well within one sector of the CD-ROM format (2352 bytes) provided the error frames are positioned within said sector. The sector comprises 98 frames, so at maximum 49 consecutive frames can have errors without

encoding errors are introduced during encoding after the C2 encoding step but before the C1 encoding step. Hence during decoding no errors at the C1 decoder are detected, and no flagging of C1 symbols occurs. However at the C2 decoding step, the errors appear and are uncorrectable. All errors can be easily controlled to be within one sector, as the interleaving and de-interleaving occurs after the C2 encoding and before the C2 decoding step. Alternatively a combination of C2 and C1 errors may be used.

The invention can be applied in systems using different error correcting rules, such as DVD. A corresponding pattern of bit errors counteracting the de-interleaving can be found according to the above description. In further applications a more sophisticated approach of error correction might be a repeated application of the error correcting rules by first interleaving the output of the first error correcting process like in the encoder and secondly de-interleave and apply the error correcting rules again. As some errors may be corrected in the first process such a second error correcting process might further correct errors. To prevent such an approach from correcting the logical errors, preferably the bit frequency and positioning of bit errors is such that they are uncorrectable in every error correcting layer.

Figure 4 shows a bit error pattern for the CIRC error correcting rules as described with Figure 3. The bit errors are designed to accumulate in the C1 error words as well as in the C2 error words, in both cases to 5 errors. The pattern of errors may be shifted to other information bytes (0-11, 16-27), but should cover only information bytes and no error correction bytes. In Figure 4 errors in bytes are indicated by the letters a,b,c,d,e, whereas bytes without errors are not marked. To affect 20 consecutive C1 words, 21 frames have been provided with errors, the odd bytes starting one frame earlier and the even frames stopping one frame later to compensate for the first delay unit 31. Due to the delays in the second delay unit 33 the errors marked by the same letter will accumulate in the C2 words, so 4 consecutive C2 frames will have 5 'e' errors, the next 4 C2 frames 5 'd' errors, up to the last 4 C2 frames with 'a' errors. No errors will be compensated because in each C1 or C2 error word either 0 or 5 errors will accumulate. This error scheme may easily be extended for more errors in more consecutive error words as required or for other interleaving rules. Also it may be applied a few times within one sector, to prevent any subsequent burst error correcting process to correct the logical errors. As mentioned above with Figure 3, the C1 corrector has a 100% detection probability of 2 and 3 error words, while 4-32 errors might occasionally be falsely corrected. Therefore a preferred embodiment using C1 errors only has 3 errors accumulating in the C1 words. An effective error pattern

record carrier. This is advantageous, in that no dedicated hardware is necessary and in that the user has all means necessary for accessing the copy protected information embodied on the record carrier.

The access control according to the invention will be effected as follows. The access control means will first acquire access control information indicative for the error pattern. This access control information may be a pattern stored on the record carrier, e.g. the licence code described with Figure 2, or an access code supplied via a network, e.g. internet or on paper. In an embodiment the error pattern may be generated using a seed value and a predefined algorithm, the seed value being stored on the copy protected record carrier. Secondly the presence of logical errors must be verified to assure that the disc is an original, copy protected disc and not an illegal copy. The access control means will select one or more error location(s) on the record carrier, or error sector(s) if the record carrier is formatted in addressable sectors, which error locations should have a logical error according to the error pattern. Thirdly the presence of an error is verified by reading the selected error location. As the reading device will generate an error message on the interface in the event that a sector to be read comprises uncorrectable errors, the presence of the logical errors can be detected effectively. As a copy will not comprise the logical errors, the copy will be rejected and the access to the information will be barred. Preferably a few error locations are selected at random from a large number of error locations available on the record carrier, e.g. in a padding area dedicated to comprise the error pattern having error sectors and non-error sectors. Alternatively the error sectors may be intermixed with valid sectors comprising normal user information. For achieving a fast response for the access control to take place, preferably only one error sector is selected and read. In practice reading one sector having uncorrectable errors might only cause a delay of a few seconds, which delay is caused by the reading device trying to read the sector a few times. Such retries are standard practice to improve the chance for successful recovery of information in the event of dirt or scratches. The error pattern may further be verified by selecting at least one non-error location, but not all non-error locations, which non-error locations should not have a logical error according to the error pattern, and verifying the absence of an error by reading the selected non-error location. As reading a non-error sector will be very fast, e.g. 0.2 seconds, a larger number of non-error sectors, e.g. 10 to 40, is preferably selected and read. Said non-error sectors are preferably selected via a random selection process from all available non-error sectors. In an embodiment the contents of the non-error sectors may be verified, e.g. by including a check value in such a sector to be derived from the sector number and the licence code by a

is modified to create the full contents 74 of the copy protected record carrier, having a logical map as described with Figure 2. A second utility provided by the licensor modifies the image file 73 by adding a licence structure including the licence number to the system area 22. The image file 73 is further be modified to pad the size of the image to include the padding area. The total length is preferably more than 74 minutes (333,000 sectors). The licence structure holds a reference to the start and end sectors of the padding area. In the padding area, sectors will either be good or bad and the distribution of the sectors will be determined by a pseudo-random process, which may be seeded from the licence number. In a fifth step 65 the image file is processed to create a master disc 75, e.g. by a Mastering House. The image file 74 is sent to the Mastering House on magnetic tape or other suitable media. Using Laser Beam Recorder software modified according to the invention a master disc 75 is produced. The Laser Beam Recorder software makes use of the licence structure to determine which sectors in the padded area are marked as being bad and which ones are good. The ratio of marked to good sectors may be fixed, e.g. approximately 50%. The errors are applied according to the error patterns described above with Figure 4. In a sixth step 66 copy protected record carriers 76, such as CD-ROM's, are produced by duplicating the master disc 75. The error pattern is transferred to each disc in this step.

Although the invention has been explained by an embodiment using the CD-ROM as example having the CIRC error correcting rules, it will be clear that other record carriers, magnetic or optical tape, etc can be employed in the invention, if such record carriers comprise information protected by predefined error protecting rules. For example, the high density DVD disc also uses an error correcting process. Whilst the invention has been described with reference to preferred embodiments thereof, it is to be understood that these are not limitative examples. Thus, various modifications may become apparent to those skilled in the art, without departing from the scope of the invention, as defined by the claims. For example, applying error patterns in error protected data transmitted via a network such as internet may provide access control according to the invention. Further, the invention lies in each and every novel feature or combination of features.

CLAIMS:

1. Method for copy protecting a record carrier having information stored thereon according to predetermined formatting and error correcting rules, comprising the steps of

(a) creating an image file comprising main information,

(b) generating access control information for controlling the access to the main information,

(c) producing a master carrier in dependence on the image file and the access control information, which producing comprises the steps of creating a bit sequence by applying the formatting and error correcting rules to the image file and translating the bit sequence into a physical pattern of marks, and

(d) multiplicating the record carrier using the master carrier,

characterized in that in step (c) bits in the bit sequence are changed according to the access control information to constitute logical errors which cannot be corrected by said error correcting rules and which constitute an error pattern.

2. Method for copy protecting a record carrier as claimed in claim 1, in which at least part of the main information is encrypted in dependence on the access control information.

3. Method for copy protecting a record carrier as claimed in claim 1, in which at least some of the access control information is included in the image file and the error pattern is generated in dependence on said included access control information.

4. Copy protected record carrier having a bit sequence stored thereon representing information according to predetermined formatting and error correcting rules, the information comprising main information and access control information for controlling the access to the main information, characterized in that the bit sequence comprises bit errors constituting logical errors which cannot be corrected by said error correcting rules and which constitute an error pattern representing at least part of the access control information.

that the record carrier is a CD, the error word correcting rule being the C2 layer and the second error word correcting rule being the C1 layer of the CD error correcting rules.

14. Method for detecting access control information on a copy protected record carrier according to any one of claims 4 to 13, characterized in that the method comprises the steps of

selecting at least one error location, but not all error locations, which error location(s) should have a logical error according to the error pattern, and

verifying the presence of an error by reading the selected error location(s).

15. Method for detecting access control information as claimed in claim 14, characterized in that the method further comprises the steps of

selecting at least one non-error location, but not all non-error locations, which non-error location(s) should not have a logical error according to the error pattern, and

verifying the absence of an error by reading the selected non-error location(s).

16. Method for detecting access control information as claimed in claim 14, characterized in that at least one non-error location is selected which adjoins an error location.

17. Method for detecting access control information as claimed in claim 14, characterized in that the method comprises a step of

retrieving at least some access control information indicative of the error pattern from the main information before selecting locations.

18. Method for detecting access control information as claimed in claim 14, characterized in that, while the record carrier is subdivided into addressable sectors, the presence or absence of an error at a location is verified by reading the respective sector and generating an error message when an uncorrectable error is detected during reading the sector.

19. Copy protected record carrier as claimed in claim 4, characterized in that the record carrier comprises software for executing the method of any one of claims 14 to 18 on a computer system.

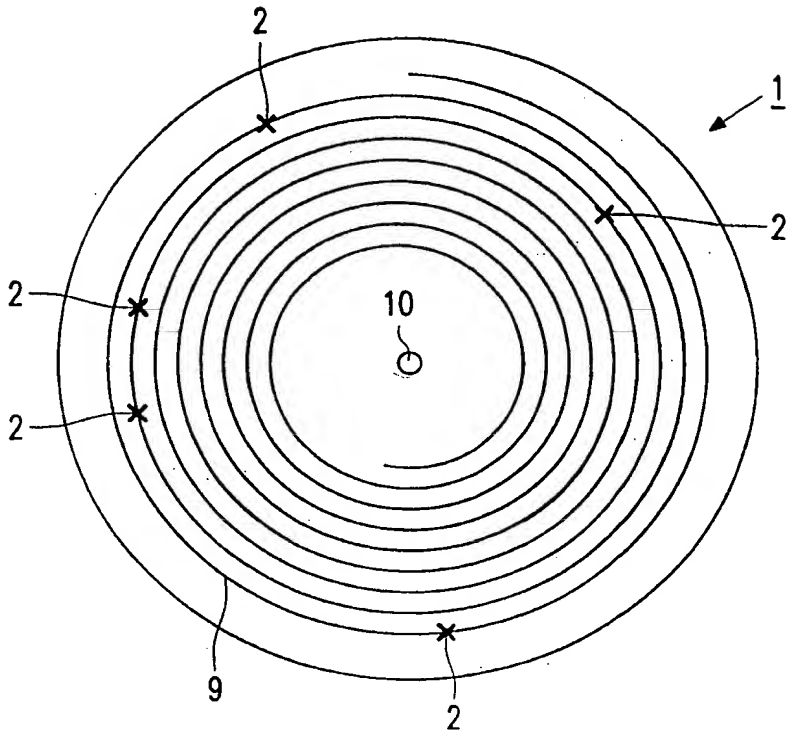

FIG. 1

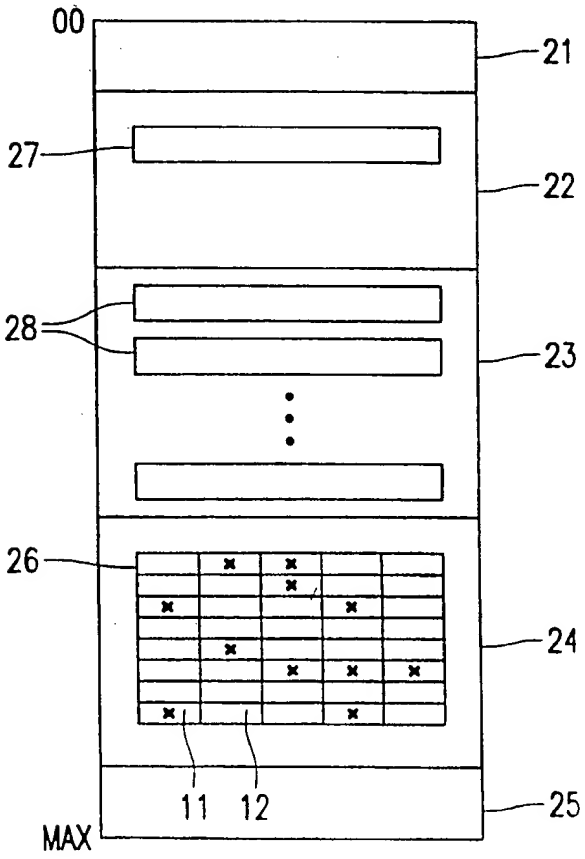

FIG. 2

BYTE NR	FRAME NUMBERS																				
									1											2	
	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
0			a	a	a	a															
1	b	b	b	b	a	a	a	a													
2			c	c	c	c	b	b	b	b	a	a	a	a							
3	d	d	d	d	c	c	c	c	b	b	b	b	a	a	a	a					
4			e	e	e	e	d	d	d	d	c	c	c	c	b	b	b	b	a	a	a	a
5					e	e	e	e	d	d	d	d	c	c	c	c	b	b	b	b	
6									e	e	e	e	d	d	d	d	c	c	c	c	c
7												e	e	e	e	d	d	d	d		
8																		e	e	e	e
9																					
..																					
31																					

FIG. 4

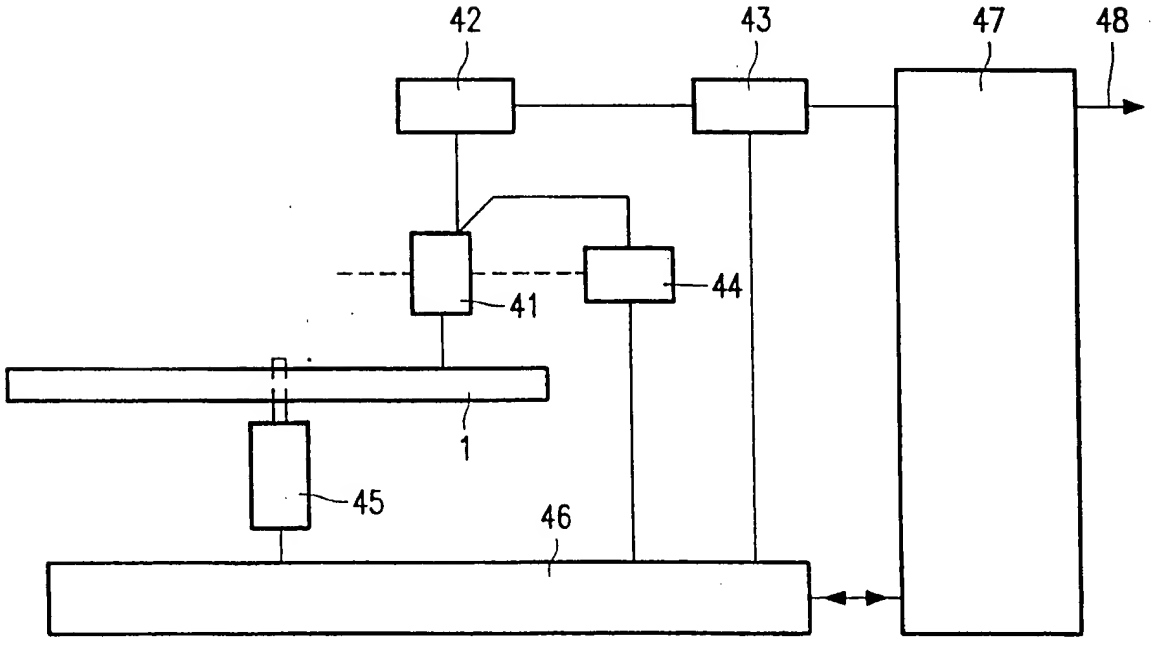

FIG. 5

INTERNATIONAL SEARCH REPORT

Inter nal Application No
PCT/IB 98/00800

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G11B20/00 G06F1/00

According to International Patent Classification(IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G11B G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PATENT ABSTRACTS OF JAPAN vol. 097, no. 006, 30 June 1997 & JP 09 044995 A (TOSHIBA CORP), 14 February 1997 see abstract	1,4,20
X	EP 0 533 204 A (OLYMPUS OPTICAL CO) 24 March 1993 see page 3, line 41 - page 7, line 5; figures 2-8	1-4,20
A	PATENT ABSTRACTS OF JAPAN vol. 096, no. 009, 30 September 1996 & JP 08 129828 A (SONY DISC TECHNOL:KK), 21 May 1996 see abstract	1,4

[ ] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 1998	21/09/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Feuer, F

Form PCT/ISA/210 (second sheet) (July 1992)